Lookout

WHITEPAPER

How to protect personal data and privacy in SAP SuccessFactors

Dynamic SaaS and cloud environments create new security challenges

Lookout CASB supports all SAP SuccessFactors modules

- Employee Central
- Performance and Goals
- Succession and Development
- Learning
- Reports
- Compensation
- Analytics
- Open Data Protocol (OData) APIs
- Workflows
- Email

Safeguard data privacy and maximize human capital management

SAP SuccessFactors revolutionized the human capital management (HCM) market, providing everything from core human resources management to advanced workforce analytics for thousands of enterprises worldwide.

Its popularity soared when legions of enterprises migrated to the cloud to benefit from the software as a service (SaaS) delivery model. This raised security concerns about protecting the confidentiality of employee information and compliance with data privacy regulations.

The security challenges are daunting. Your apps have left the building. Employees work remotely using devices and networks you don't control. There are no fixed perimeters in the cloud. Data must be available everywhere.

The challenges deepened with the emergence of international data residency and privacy laws. According to the law firm of Morrison and Foerster, 133 jurisdictions worldwide had enacted data privacy laws as of January 2021.

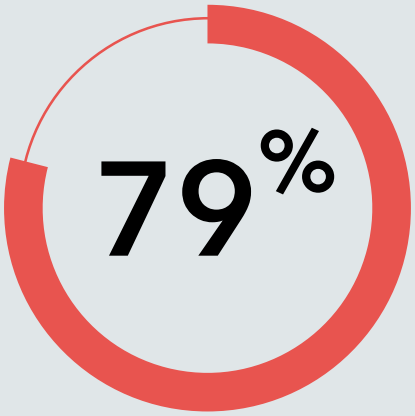
As a result, enterprises that invest in SuccessFactors must secure all data – from mobile endpoints to cloud-hosted SaaS – and reduce business risk by protecting personally identifiable information (PII), protected health information (PHI) and other confidential information in accordance with privacy regulations.

The Lookout® CASB – a cornerstone of our integrated endpoint-to-cloud security platform – does exactly that. We give you detailed visibility into your entire security infrastructure, along with dynamic access controls, data protection, cyberthreat detection and compliance management.

With Lookout CASB, you can be confident that the privacy of employee data is protected across all fronts – spanning human resources, payroll, recruiting, workforce planning, and other strategic HCM business processes.

SuccessFactors data security checklist

- ✓ Extend visibility into SAP SuccessFacvtors cloud usage.
- ✓ Enable Zero Trust access from any device and location.
- ✓ Enforce advanced data protection policies to detect, classify and secure sensitive data.
- ✓ Apply Zero Trust encryption with 100% ownership of encryption keys.
- ✓ Secure downloaded data with enterprise digitalrights management.
- ✓ Monitor user activity to identify anomalous behaviour and threats.
- ✓ Support complex global compliance requirements to ensure data privacy.



"79 percent of organizations have experienced an identity-related breach in the last two years, and 99 percent believe their identity-related breaches were preventable."

Identity Defined Security Alliance
May 2020

Protect data by using detection and classification

Before human resources processes connect to SuccessFactors, user identities must be verified before granting access. The widespread use of personal devices for work underscores the importance of identity- and context-aware access to apps.

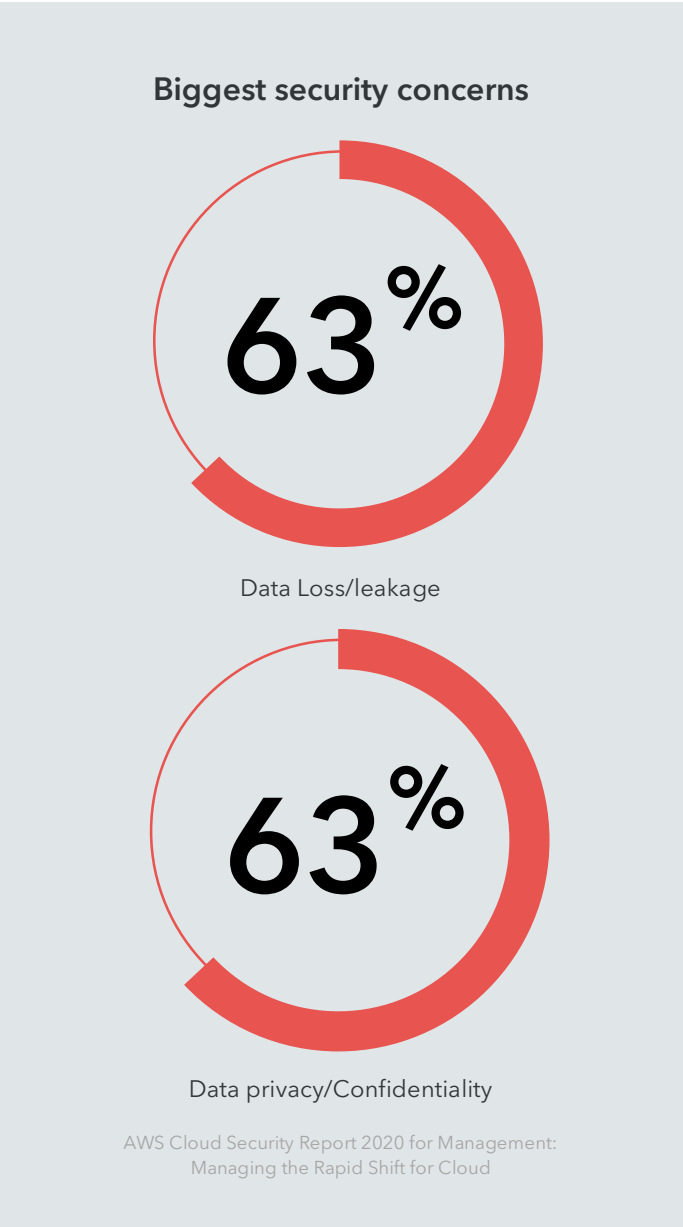
Lookout CASB lets you define granular, context-aware policies for Zero Trust access to data hosted in SuccessFactors. Policies are enforced by using a combination of contextual factors and step-up authentication that prompts workers to provide additional credentials to ensure policy compliance.

Contextual factors employed by Lookout CASB include user identity, user group, location, IP address, devices, operating systems, baselines of user behaviors, device compliance and intellectual property risk.

Additional capabilities

- ***Integrates with mobile device management (MDM) and enterprise mobility management (EMM)*** – Lookout CASB enforces device access-restrictions after retrieving and classifying endpoint devices as managed or unmanaged. This prevents users from downloading salary reports and other confidential data to unmanaged devices.
- ***Integrates with identity providers*** – In reverse-proxy mode, Lookout CASB integrates with Microsoft Azure AD, Okta, Ping and Thales to enforce Zero Trust from devices and locations to authorized cloud apps. Identity, coupled with single sign-on and multifactor authentication (MFA), give you granular access controls for SaaS app log-in activities.
- ***Preventing unauthorized access***– Lookout CASB detects and blocks suspicious login times and locations, such as identifying a user's attempt to log-in from overseas only two hours after the same user authenticated from North America.

Protect data by using detection and classification



To boost productivity across HCM processes, you must first protect the PII and other confidential data that is uploaded to SuccessFactors and shared with connected third-party apps. This ensures secure connections for employees, business partners and contractors who use managed and unmanaged devices from any location.

CASB gives you the strongest data protections and access controls available for SuccessFactors. We continuously ensure the integrity and fidelity of data in motion and data at rest across all SAP modules for SuccessFactors.

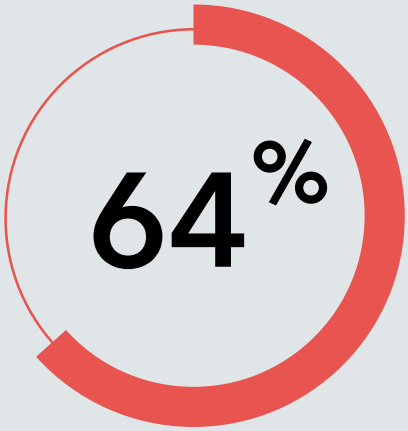
Lookout data protection for SuccessFactors

DLP extends data protection and access controls to SuccessFactors in the cloud. You can create granular policies that scan sensitive data in real-time for assigned classification, rules enforcement, encryption, masking, watermarking, quarantining or deletion.

Policy creation options – Options include allow or deny uploads, logging, notification, denial, protect bulk data imports, step-up authentication, apply data classification labels, encrypt files to protect data during downloads, user compliance coaching, document highlighting, redaction, watermarking, permanent deletion and user remediation.

Field and file-level data protection – Lookout CASB protects SuccessFactors field-level data (structured) and unknown files or notes (unstructured). Protected fields include personal employee records and extend further to names, addresses, phone numbers, email addresses and social security numbers. Custom fields can also be protected to encrypt sensitive industry-specific data, such as Military IDs.

Data classification – Lookout CASB classifies data while providing visibility into and protection across SuccessFactors modules and apps, users and devices. This protects employee records and sensitive data from unintended exposure. We also integrate with Microsoft Information Protection (MIP) and Titus to extend data classification and governance to any document in any cloud.



"Over 64% of financial services companies have 1,000 sensitive files open to every employee."

Varonis
2021 Financial Services Data Risk Report

Apply Zero Trust encryption with exclusive key control

Although some SaaS providers protect at-rest data, such as in storage, most do not secure in-use data and in-transit data. This can leave sensitive and confidential clear-text information in SaaS apps vulnerable to devastating data breaches.

Additionally, many cloud app key management policies and processes might not comply with GDPR, HIPAA and CCPA data protection laws because SaaS providers – not their customers – control encryption keys.

Lookout CASB Zero Trust encryption for SuccessFactors offers the most compelling approach to data protection. It provides tighter controls over SuccessFactors HCM modules within apps.

We use 256-bit AES encryption to protect PII in SuccessFactors while preventing unencrypted data from leaving your network. You exclusively retain valid encryption keys to prohibit unauthorized users, cloud provider system administrators and outsiders from accessing data without permission.

Unique benefits of Lookout CASB encryption

Hold your own keys – Lookout CASB key management gives you sole ownership of keys to encrypt data. SuccessFactors does not possess keys, decrypt data or share it with any third-party app, which stops unauthorized data disclosures.

Format preservation – Strong encryption from Lookout CASB preserves field-level policy formats in SuccessFactors. We also deliver partial field encryption when searching, sorting, reporting and charting data. This empowers you with best-in-class data protection and without interfering with critical HCM processes.

Secure downloaded data with enterprise digital rights management

"There are undeniable risks in permitting employees' access to corporate resources from personal devices."

Forbes

The growing number of employees who are using personal mobile devices for work creates new challenges to protect confidential data as it travels outside the cloud environment, extending the need for secure offline data access.

Enterprise Digital Rights Management (E-DRM) in Lookout CASB applies strong protection controls to confidential data in SuccessFactors. We automatically encrypt personal information about employees, salary reports and related workflows during downloads to user devices for last-mile data protection.

You can define EDRM policies to permit file access and downloads on managed devices only and restrict access to authorized users who are granted permission to decrypt downloaded files using the Lookout CASB lightweight EDRM client.

Additional EDRM protections

Full visibility and data ownership – Lookout CASB gives you complete visibility into any data accessed and downloaded by internal and external users, including customers, vendors, and partners. We empower you to control downloaded files, regardless of where they are being shared.

Decryption key management – Lookout CASB lets you revoke decryption keys and stop user access in real-time to protect confidential data on lost or stolen devices. This also protects data from misuse, such as preventing former employees from taking customer data to new companies.

Identify anomalous user behaviors and cyberthreats

Any SaaS platform – SuccessFactors included – can fall victim to malware that will initiate a cyberattack that spreads laterally throughout your cloud infrastructure, propagates to other clouds and bypasses conventional antivirus systems.

These cybercriminals typically use command-and-control tactics to compromise devices and apps and hijack personal and administrative login credentials. Access privileges continue to escalate until they find confidential data and valuable intellectual property, which results in a catastrophic data breach.

Lookout CASB addresses this manner of cybersecurity threat by aggregating and correlating related data from across enterprise networks, clouds, SaaS and mobile environments. We give you full visibility into the earliest signs of threat behaviors so you can quickly mitigate attacks and stop data breaches.

"The average cost to recover from a cyberattack for organizations with more than $1 billion in revenue is $4.6 million."

TechBeacon

Detect suspicious behaviors and cyberthreats

Zero-day threat protection – Integrated antivirus/antimalware (AV/AM) in Lookout CASB scans all inbound and outbound cloud content to defend against viruses, malware and ransomware with industry-leading detection rates. Infected content is quarantined on the fly without noticeable latency.

Additionally, URL link protection and on-premises sandbox integration enable you to quickly detect and remediate today's most advanced cyberthreats.

User and entity behavior analytics – User and entity behavior analytics (UEBA) in Lookout CASB leverages sophisticated machine learning algorithms to monitor activity in SuccessFactors, including unusual region or time of day, attempted bulk file downloads, and other anomalous behaviors.

UEBA provides real-time alerts about anomalous behaviors that might originate from a cyberattacker or malicious worker. In this case, Lookout CASB will block actions based on variations in normal behavioral patterns.

Examples of these anomalies include an abnormally large number of downloads from an individual user, an unusually high volume of login attempts from the same user or persistent login attempts by an unauthorized account.

SIEM support – Lookout CASB extends user activity logs collected on-premises to the cloud by integrating with Microfocus ArcSight, IBM QRadar, Intel Security, LogRhythm, and Splunk SIEMs. This enables you to combine incident management automation with centralized analysis and reporting of endpoint-to-cloud security events.

Ensure regulatory compliance to protect data privacy and residency

"By 2023, 65% of the world's population will have its personal information covered under modern privacy regulations, up from 10% today."

Gartner Report: The State of Privacy and Personal Data Protection, 2020-2022

Data protection laws like GDPR require you to prevent personal data from being retained in or traveling through countries that do not have data protection standards that are equivalent to the resident country.

This creates a complex global challenge for organizations that rely on SuccessFactors and other SaaS app platforms. Cloud services often involve multiple data centers that are geographically dispersed among several regions to ensure high availability and minimize latency.

Lookout CASB uses cloud encryption gateways to provide secure, centralized compliance and governance. This includes absolute data residency, protection from government forced disclosure, and safe harbor from breach notifications.

Centralized compliance and governance

Absolute data residency – Lookout CASB encryption and key management allow one global instance of a SaaS app and selectively encrypts and tokenizes data for each required country to meet local residency requirements. This absolute capability for data-residency control ensures that PII and confidential data from SuccessFactors are not revealed outside of the country or area of sovereignty.

Protection from government forced disclosure – Lookout CASB delivers a unique and powerful key management capabilities that always remains under your control and jurisdiction. This prevents access through forced government disclosures and empowers you with 100 percent control over data access.

Safe harbor from breach notification – Data most often cannot be breached if it is encrypted and if related data encryption keys reside solely with you. Under most compliance regulations, you are not required to notify your customers or employees if a cyberattacker or malicious insider gets hold of encrypted data, which protects reputational risk and eliminates the cost associated with a publicly disclosed breach.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.